CLAIMS

What is Claimed is:

1. In a Montgomery multiplication algorithm, a method of computing an output xyR^{-1} mod m from input integers $m = (m_{n-1} \ldots m_1 m_0)_b$, $x = (x_{n-1} \ldots x_1 x_0)_b$, $y = (y_{n-1} \ldots y_1 y_0)_b$, with $0 \le x, y < m$, $R = b^n$ with gcd(m, b) = 1, and $m' = -m^{-1}$ mod b comprising the steps of:

representing a value A in the Montgomery multiplication algorithm with a redundant notation; and

performing carry-save addition within an iterative process of the Montgomery multiplication algorithm to compute a new value of A.

2. The method of Claim 1, further comprising executing the algorithm:

a. $S \leftarrow 0$ and $T \leftarrow 0$ (where $S = (s_n s_{n-1} \ldots s_1 s_0)_b$ and $T = (t_n t_{n-1} \ldots t_1 t_0)_b$.)

b. For i from 0 to (n-1), do the following:

b1. $u_i \leftarrow (s_0 + t_0 + x_i y_0)\, m' \bmod b$

b2. $(S, T) \leftarrow (S + T + x_i y + u_i m) / b$

c. $A_1 \leftarrow S + T$ and $A_2 \leftarrow S + T - m$

d. If $A_2 \ge 0$ then $A \leftarrow A_2$ else $A \leftarrow A_1$

e. Return A

3. The method of Claim 2, wherein the value of b is two.

4. The method of Claim 2, wherein step b2 of the algorithm further comprising selecting one of $y+m$, y, m, or 0 to be added to S and T.

5. The method of Claim 1, wherein said representing step further comprises replacing said value of A with two other values, wherein a sum of the other two values equals said value of A.

6. The method of Claim 1, wherein said performing step further comprises performing said carry-save addition in parallel.

7. The method of Claim 1, wherein said performing step further comprises executing said iterative process a plurality of times equal to a number of bits representing said value of x.

8. A method of performing a Montgomery exponentiation of x^e mod m wherein the notation Mont(x, y, m) denotes the Montgomery multiplication algorithm yxR^{-1} mod m from input integers $m = (m_{n-1} \ldots m_1 m_0)_b$, $x = (x_{n-1} \ldots x_1 x_0)_b$, $y = (y_{n-1} \ldots y_1 y_0)_b$, with $0 \leq x, y < m$, $R = b^n$ with gcd(m, b) = 1, and $m' = -m^{-1}$ mod b comprising the steps of:

representing a value A in the Montgomery multiplication algorithm with a redundant notation; and

performing carry-save addition within an iterative process of the Montgomery multiplication algorithm to compute a new value of A.

9. The method of Claim 8, wherein m has s bits, e has t+1 bits, and 0<x<m, and the Montgomery exponentiation is performed according to the algorithm:

a. Compute $R = b^s$

b. Compute R*R mod m

c. Compute z = Mont(x, R*R mod m, m)

d. Compute B = R mod m

e. For i from t to 0 do the following:

e.1 B = Mont (B, B, m)

e.2 If $e_i = 1$ then B = Mont (B, z, m)

f. B = Mont (B, 1, m)

g. Return B.

10. The method of Claim 8, further comprising executing the algorithm for Mont (x, y, m):

a. S ← 0 and T ← 0 (where S = $(s_n s_{n-1} \ldots s_1 s_0)_b$ and $T = (t_n t_{n-1} \ldots t_1 t_0)_b$.)

b. For *i* from 0 to (*n*-1), do the following:

b1. $u_i \leftarrow (s_0 + t_0 + x_i y_0)\, m' \bmod b$

b2. $(S, T) \leftarrow (S + T + x_i y + u_i m) / b$

c. $A_1 \leftarrow S + T$ and $A_2 \leftarrow S + T - m$

d. If $A_2 \geq 0$ then $A \leftarrow A_2$ else $A \leftarrow A_1$

e. Return *A*

11. The method of Claim 10, wherein the value of b is two.

12. The method of Claim 10, wherein step b2 of the algorithm further comprising selecting one of *y*+*m*, *y*, *m*, or 0 to be added to *S* and *T*.

13. The method of Claim 8, wherein said representing step further comprises replacing said value of *A* with two other values, wherein a sum of the other two values equals said value of *A*.

14. The method of Claim 8, wherein said performing step further comprises performing said carry-save addition in parallel.

15. The method of Claim 8, wherein said performing step further comprises executing said iterative process a plurality of times equal to a number of bits representing said value of *x*.

16. The method of Claim 8, further comprising solving a plurality of Montgomery multiplication problems simultaneously.

17. The method of Claim 16, and further comprising controlling selection of values to be added to S and T corresponding to each said of said plurality of Montgomery multiplication problems.

18. An apparatus for performing a Montgomery multiplication for an output of xyR^{-1} mod m and an input of $m = (m_{n-1} \ldots m_1 m_0)_b$, $x = (x_{n-1} \ldots x_1 x_0)_b$, $y = (y_{n-1} \ldots y_1 y_0)_b$, with $0 \leq x, y < m$, $R = b^n$ with gcd(m, b) = 1, and $m' = -m^{-1}$ mod b, comprising:

a plurality of storage units, with each one of the plurality of storage units corresponding to a value of x, m, y, S and T, where $A = S + T$, wherein the corresponding storage unit for x can shift its value, and the corresponding storage units for S and T can be set to zero;

an adder configured to add the k terms from x_i times y, the k terms from u_i times m, and S and T; and

a carry look-ahead adder configured to add any one set of values from a group including S and T, and S shifted and T shifted.

19. The apparatus of Claim 18, wherein for b greater than or equal to two, the adder further comprises a carry-save adder within an iterative process of the Montgomery multiplication algorithm to compute a new value of A.

20. The apparatus of Claim 19, wherein said carry-save adder further comprises a Wallace tree.

21. The apparatus of Claim 18, wherein b is equal to two.

22. The apparatus of Claim 21, wherein the adder further comprises a full adder configured to add input values of S, T, and any one value from a group consisting of m, y, $m+y$, zero, and $\sim m$ to produce a sum value and a carry value.

23. The apparatus of Claim 18, wherein said plurality of storage units and said added are operatively coupled to execute the algorithm:

a. $S \leftarrow 0$ and $T \leftarrow 0$ (where $S = (s_n s_{n-1} \ldots s_1 s_0)_b$ and $T = (t_n t_{n-1} \ldots t_1 t_0)_b$.)

b. For i from 0 to $(n-1)$, do the following:

b1. $u_i \leftarrow (s_0 + t_0 + x_i y_0)\, m' \bmod b$

b2. $(S, T) \leftarrow (S + T + x_i y + u_i m) / b$

24. The apparatus of Claim 23, wherein said carry look-ahead adder is adapted to execute the algorithm:

c. $A_1 \leftarrow S + T$ and $A_2 \leftarrow S + T - m$

d. *If* $A_2 \geq 0$ *then* $A \leftarrow A_2$ *else* $A \leftarrow A_1$

25. The apparatus of Claim 23, wherein the storage units corresponding to said value of x, y, m, y+m, S, and T are further adapted to hold a plurality of Montgomery multiplication problems that are solved simultaneously, and further comprising means for controlling the selection of values to be added to S and T corresponding to each said of said plurality of Montgomery multiplication problems.

26. The apparatus of Claim 25, wherein for each of said plurality of Montgomery multiply problems, the carry look-ahead adder is adapted to execute the algorithm:

c. $A_1 \leftarrow S + T$ *and* $A_2 \leftarrow S + T - m$

d. *If* $A_2 \geq 0$, *then* $A \leftarrow A_2$, *else* $A \leftarrow A_1$.